A feasible quantum communication complexity protocol

Ernesto F. Galvão
Centre for Quantum Computation, Clarendon Laboratory,
Univ. of Oxford, Oxford OX1 3PU U.K.

June 22, 2001

Abstract

I show that a simple multi-party communication task can be performed more efficiently with quantum communication than with classical communication, even with low detection efficiency η. The task is a communication complexity problem in which distant parties need to compute a function of the distributed inputs, while minimizing the amount of communication between them. A quantum optical setup is suggested that can demonstrate a 5-party quantum protocol with higher-than-classical performance whenever $\eta > 0.25$.

In theory, quantum communication is better than classical communication. Experimentalists, on the other hand, know that even the simplest quantum communication protocols involve inefficiencies in state preparation, manipulation and measurement. It is, therefore, important to study sufficient experimental conditions for unambiguous demonstration of the advantages of quantum communication. Some tasks are only possible with quantum communication, such as unconditionally secure cryptographic key distribution [1, 2, 3]. Many authors have analyzed the experimental requirements for the security of these protocols [4, 5, 6]. For other tasks quantum communication offers an improvement of efficiency, and such is the case of.communication complexity problems [7, 8], one of which will be analyzed in this letter. In these problems many distant parties need to compute a function of the distributed inputs, while trying to minimize the amount of communication between them. This abstract problem has numerous practical applications, for example in computer networks, VLSI circuits and data structures (see [8] for a survey of the field).

Quantum mechanics can enhance the performance of communication complexity protocols in two different ways [9]. The first approach is the *entanglement-based* model of communication complexity [10, 11, 12, 13], where in addition to the classical communication we allow the parties to do measurements on previously shared multi-party entangled states. Experimental requirements for some protocols of this kind have been studied in [14, 15], and it turns out that the high detection efficiency needed could be achieved in ion trap experiments [16].

The second way to obtain a genuine quantum advantage is to allow the parties to exchange qubits instead of classical bits [17, 18]. That such a *quantum communication* model may be superior to the classical case is surprising, given the results of Holevo [19] and Nielsen [20, 18] that state that no more than n bits of expected information can be transmitted by n qubits, if the parties start off unentangled. Despite the many theoretical results obtained by different authors [9], to date no experiment has been performed to demonstrate the superiority of quantum communication for this kind of distributed computation task. In this letter I propose a feasible quantum optical experiment which implements a quantum protocol with higher-than-classical performance for a specific communication complexity task. The quantum advantage is shown to arise from the use of a quantum phase to encode information. It is sufficient to have a single-photon detection efficiency $\eta > 0.25$ for the quantum protocol to outperform any classical protocol for the same problem.

The communication complexity problem we will tackle is the *Modulo-4 Sum* problem defined for three parties by Buhrman, Cleve and van Dam [12], and later generalized to N parties ($N \geq 3$) in [13]. The problem can be stated as follows. Each party P_i receives a two-bit string input x_i, subject to the constraint:

$$\left(\sum_{i=1}^{N} x_i \right) \bmod 2 = 0. \tag{1}$$

The strings are chosen randomly with an uniform probability distribution among those combinations that satisfy eq. 1 above. After some communication between the parties, one of them (say the last one P_N) must compute the value of the Boolean function

$$F(\overrightarrow{x}) = \frac{1}{2} \left[\left(\sum_{i=1}^{N} x_i \right) \bmod 4 \right]. \tag{2}$$

In other words, each party is given a number $x_i \in \{0, 1, 2, 3\}$, subject to the constraint that the sum of all x_i is even. After some communication the last party must decide whether the sum modulo-4 is equal to 0 or 2.

References [12, 13] dealt with this problem in the entanglement-based model of communication complexity, showing that the amount of classical communication necessary to compute F (on inputs constrained by eq. 1) can be decreased if the parties are allowed to do local measurements on N-party Greenberger-Horne-Zeilinger (GHZ) states

$$|GHZ\rangle = \frac{1}{\sqrt{2}} \left(|0_1 0_2 \cdots 0_N\rangle + e^{i\phi} |1_1 1_2 \cdots 1_N\rangle \right). \tag{3}$$

When considering the quantum communication model, we must limit the amount of bits (qubits) to be exchanged between the parties and compare the success rates obtained by the optimal classical and the quantum protocols. The criterion for a successful demonstration of better-than-classical communication is simple: we just need to obtain an experimental quantum success rate which is better than that of the optimal classical protocol.

Let us limit the amount of communication to $(N-1)$ bits (or qubits). Another constraint we impose is that the communication must be *sequential*, in which party P_1 can only send information to party P_2, who in turn can only send a message to party P_3 and so on until party P_N, who then computes F. The decision to demand sequential communication is related to the fact that the sequential quantum communication necessary to solve this problem can be conveniently realized by sending a single photon through a series of optical elements representing the parties.

First, let us obtain the optimal classical success rate for the Modulo-4 Sum problem, with only $(N-1)$ bits of sequential classical communication. We start by noting that if one of the parties (say party P_j) sends no information to party P_{j+1}, then party P_N cannot compute F correctly with probability $p_c > 1/2$. This is so because such a break in the communication flow would leave party P_N with no information about the numbers $x_1, x_2, ..., x_j$, and there are as many allowed j-tuples $(x_1, x_2, ...x_j)$ resulting in $F(\overrightarrow{x}) = 1$ as in $F(\overrightarrow{x}) = 0$. Therefore, in order to obtain a performance which is better than a random guess, each party P_j must send exactly one bit to the next party P_{j+1} .

For the moment let us consider only deterministic protocols. The first party P_1 has access only to her two-bit string x_1, and so can choose between 2^4 protocols. These can be represented by the four-bit string $prot_1$, whose n^{th} $(n = 0, 1, 2, 3)$ bit encodes the message m_1 to be sent to P_2 if $x_1 = n$. The other parties P_j $(j = 2, ..., N-1)$ can choose among 2^8 protocols that take into consideration both x_j and the message m_{j-1} received from the previous party. Each of these protocols can be represented by an 8-bit string $prot_j$, whose n^{th} $(n = 0, 1, ..., 7)$ bit encodes the message to be sent when $x_j + 2m_{j-1} = n$.

Each possible deterministic protocol can then be represented by the $(N-1)$-tuple $\overrightarrow{prot} = (prot_1, prot_2, ..., prot_{N-1})$. Finding the probability of success of a given protocol $\overrightarrow{prot}$ is a straightforward computation. We start by producing a list of all possible input data $\{x_1, x_2, ..., x_{N-1}\}$ compatible with $x_N = 0$, computing the messages m_{N-1} corresponding to each, and finding the fraction of cases in which P_N's most likely guess about F would in fact be correct. This is repeated for $x_N = 1, 2$ and 3, and the results averaged to obtain the overall probability of success p_c. The optimal deterministic protocol can then be found by a computer search over all $2^4(2^8)^{N-2} = 2^{(8N-12)}$ protocols.

For number of parties $N = 3, 4$ and 5 I obtained the optimal classical probability of success

$$\begin{aligned} p_c^{N=3} &= 3/4, \\ p_c^{N=4} &= 3/4, \\ p_c^{N=5} &= 5/8. \end{aligned} \tag{4}$$

A limited search over protocols for larger number of parties yields some lower bounds for p_c:

$$p_c^{N=6} \geq 5/8,$$
$$p_c^{N=7} \geq 9/16,$$
$$p_c^{N=8} \geq 9/16.$$

The optimal p_c for $N = 3, 4$ and 5 is attained by many protocols, for example the one consisting of $prot_0 = 0011$ and all the other $prot_j = 01011010$. The same protocol yields the lower bounds for the optimal probabilities of success presented above for $N = 6, 7$ and 8. Checking that these lower bounds are tight would involve a prohibitively long exaustive search over all protocols. For the purpose of comparison with the quantum protocol given below, it would be enough to obtain an analytical upper bound for p_c^N that decreases with N. Unfortunately I could not prove such a general result, despite the symmetries of the problem.

Up to now we have been computing the probability of success for deterministic classical protocols. In a probabilistic protocol, each party P_j would choose among protocols $prot_j$ according to some random numbers. However, any such probabilistic protocol can be turned into a deterministic one by having the parties share the random numbers before they are given their input data. Therefore, the optimal classical probability of success p_c obtained above is an upper bound for the performance of any classical protocol, deterministic or not. This point has been discussed at length in chapter 3 of the book by Kushilevitz and Nisan [8].

We have seen that the Modulo-4 Sum problem gets harder and harder to solve classically, as the number of parties increases. There is, however, a simple quantum protocol with sequential qubit communication that has a probability of success $p_q = 1$ *independently* of the number of parties involved. The idea is to start with the qubit in state

$$|\psi_i\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right)$$

and send it flying by all the parties, from first to last. Each party needs only act upon the qubit with a phase operator $\phi(x_j)$, defined as

$$\phi(x_j) = \left\{ \begin{array}{c} |0\rangle \rightarrow |0\rangle \\ |1\rangle \rightarrow e^{i\frac{\pi}{2}x_j}\,|1\rangle \end{array} \right. , x_j = \{0, 1, 2, 3\}. \tag{5}$$

After going through the N phase operations the qubit state will be

$$|\psi_f\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{F(\overrightarrow{x})}\,|1\rangle\right),$$

due to the constraint 1 on the possible inputs x_j. The last party can then measure $|\psi_f\rangle$ in the $\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle\}$ basis, obtaining F with probability $p_q = 1$.

The protocol above is an adaptation of the entanglement-based protocol presented in [13] to the qubit-communication setting. In the entanglement-based protocol each party performs a phase operation and measurement on his/her qubit of the N-party GHZ state they share. The value of the function F is encoded in the quantum phase ϕ (see eq. 3), by individual phase shifts applied by each party on his/her particle.The last party P_N obtains the value of F from the results of the N measurements (hers plus the $N-1$ broadcast to her by the other parties). The probability of success is $p_q = 1$ only when all the N detections are successful, hence the high detection efficiencies required for a higher-than-classical performance [15]. Here we obtain the same performance by using the phase of a *single* qubit to acquire information on F as it flies by the parties towards the last party P_N, where a single detection reveals the result.

The detection efficiency η must still be taken into account, as it lowers the probability of success of the quantum protocol. In case of a successful detection (which occurs with probability η) the probability of success is equal to one. In case the detection fails (probability $1-\eta$), the last party P_N has to make a random guess about the value of F, succeeding only with probability 1/2. Thus for a higher-than-classical performance we need to implement the quantum protocol with a detection efficiency η such that

$$\eta + (1-\eta)\frac{1}{2} > p_c. \tag{6}$$

Thus, it is sufficient to have $\eta > 2p_c - 1$. We have seen that the optimal classical protocol for $N = 5$ parties has a success rate $p_c^{N=5} = 5/8$, and therefore can be beaten by the quantum protocol if the detection efficiency $\eta > 0.25$. It is interesting to note that even lower detector efficiencies might be sufficient if one can prove that $p_c^N < 5/8$ for some $N > 5$.

The quantum protocol for the Modulo-4 Sum problem can be demonstrated with a simple quantum optical setup. The flying qubit is encoded in the polarization state of a single photon. For a fair comparison with the classical protocol, it is important to allow only a single photon per run to pass by the parties and arrive at P_N. This can be achieved by using a parametric down conversion crystal pumped by a laser. Detection of one of the twin photons generated can be used as a trigger to let the second photon go towards the parties. For the triggering mechanism to work we need to introduce a delay for the second photon, which can be easily achieved by coupling it to a few meters of optical fiber. Upon detection of the first photon, the second photon is allowed to come through the N parties. Each party consists of an optical element using birefringent materials to perform the phase shift given by eq. 5. In the end, the last party P_N must also detect the photon in the proper basis. Since there is very little loss at each of the parties, the only significant limitation in this implementation of the quantum protocol is the detector efficiency. There exist high efficiency single photon detectors with $\eta \simeq .55$ at certain wavelengths [21], sufficient for a successful demonstration of the quantum protocol for $N = 5$ parties.

It is clear that essentially the same setup can be used to solve the Modulo-4 Sum problem using classical polarized light. In common with a qubit, classical light has a continuous variable (the phase) that can be manipulated, as opposed to classical bits that can only assume two discrete values. The counter-intuitive quantum feature that helps in communication complexity is the fact that even single photons still retain the continuous description of the classical electromagnetic field. More generally, a d-dimensional pure quantum state is characterized by $2(d-1)$ real parameters that can be used for communication purposes, as opposed to the d discrete states available to a classical system of same dimensionality. Defining exactly for which communication tasks such a different resource can be used to advantage is a central research problem in quantum information theory.

In summary, I have shown that an experimental demonstration of a communication complexity protocol is feasible using a simple quantum optical setup with photon detection efficiency of at least 25%. The higher-than-classical performance of the quantum communication protocol arises directly from the use of a quantum phase to encode information. If implemented, this would be the first experiment to demonstrate the superiority of quantum communication over classical communication for distributed computation tasks.

I would like to thank Lucien Hardy for fruitful discussions and for his support and encouragement. I would also like to thank Antia Lamas-Linares for helpful discussions about quantum optics experiments. I acknowledge support from the U.K. Overseas Research Studentships scheme and from the Brazilian agency Coordenação de Aperfeiçoamento de Pessoal de Nivel Superior (CAPES).

References

[1] C. H. Bennett and G. Brassard, in *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing*, Bangalore, India (1984), pp. 175-179.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] C. H. Bennett, Phys. Rev. Lett. **67**, 661 (1992).

[4] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[5] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[6] H. Aschauer and H. J. Briegel, LANL preprint quant-ph/0008051 (2000).

[7] A. C. Yao, in *Proc.11th Ann. ACM Symp. on Theory of Computing* (1979), pp. 209-213.

[8] E. Kushilevitz and N. Nisan, *Communication Complexity*, Cambridge University Press, 1997.

[9] G. Brassard, LANL preprint quant-ph/0101005 (2001).

[10] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997).

[11] L. K. Grover, LANL preprint quant-ph/9704012 (1997).

[12] H. Buhrman, R. Cleve and W. van Dam, LANL preprint quant-ph/9705033 (1997).

[13] H. Buhrman *et al.*, Phys. Rev. A **60**, 2737 (1999).

[14] W. van Dam, *Non-locality & Communication Complexity*, PhD Thesis, Department of Physics, University of Oxford (1999).

[15] E. F. Galvão, LANL preprint quant-ph/0009014 (2000).

[16] M. A. Rowe *et al.*, Nature **409**, 791 (2001).

[17] A. C. Yao, in *Proc. of the 34th Ann. IEEE Symp. on Foundations of Computer Science* (1993), pp 352-361.

[18] R. Cleve, W. van Dam, M. Nielsen and A. Tapp, in *Quantum Computing and Quantum Communication: Proceedings of First NASA International Conference*, Lecture Notes in Computer Science, vol. 1509, Springer-Verlag (1999), pp 61-74.

[19] A. Holevo, *Problemy Peredachi Informatsii* **9**, no. 3 (1973), pp. 3-11. English translation in *Problems of Information Transmission* **9** (1973), pp. 177-183.

[20] M. A. Nielsen, *Quantum Information Theory*, PhD Thesis, Department of Physics, University of New Mexico (1998). Available as a LANL preprint quant-ph/0011036.

[21] C. Kurtsiefer *et al.*, LANL preprint quant-ph/0104113 (2001).